IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: François GRIEU
Grégory MARDINIAN

Serial No:

Filed:

For: A METHOD OF INTERCHANGING DATA BETWEEN AN AUTOMATIC MACHINE AND A PORTABLE OBJECT, IN PARTICULAR A MICROCIRCUIT CARD, THE OBJECT BEING SUITABLE FOR DEBITING BY THE MACHINE IN CONSIDERATION FOR PROVIDING GOODS OR SERVICE

**DECLARATION**

I, Andrew Scott Marland, of 35, avenue Chevreul, 92270 BOIS COLOMBES, France, declare that I am well acquainted with the English and French languages and that the attached translation of the French language PCT international application, Serial No. **PCT/FR99/02470** is a true and faithful translation of that document.

All statements made herein are to my own knowledge true, and all statements made on information and belief are believed to be true; and further, these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any document or any registration resulting therefrom.

Date: March 2, 2001

Andrew Scott Marland

PCT/FR 99/02470

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION

09/806907

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION



## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 15 OCT. 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA REGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30



ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

# BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

## REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 13 OCT. 1998

N° D'ENREGISTREMENT NATIONAL 98 12770

DÉPARTEMENT DE DÉPÔT 75

DATE DE DÉPÔT 13 OCT. 1998

**1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE**

Dominique DUPUIS-LATOUR
Avocat à la Cour
Cabinet BARDEHLE, PAGENBERG & PARTNER
45, avenue Montaigne
75008 - PARIS

n°du pouvoir permanent — références du correspondant 464-I 51247-FR — téléphone 01 44 43 91 99

**2 DEMANDE** Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Procédé d'échange de données entre un automate et un objet portatif, notamment une carte à microcircuit, susceptible d'être débité par l'automate en contrepartie de la délivrance d'un bien ou d'un service.

**3 DEMANDEUR (S)** n° SIREN code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

INNOVATRON ELECTRONIQUE

Forme juridique

Société Anonyme

Nationalité (s) Française

Adresse (s) complète (s) Pays

, rue Danton
75006 - PARIS

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

**4 INVENTEUR (S)** Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

**5 RÉDUCTION DU TAUX DES REDEVANCES** ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

**6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE**

| pays d'origine | numéro | date de dépôt | nature de la demande |
|---|---|---|---|
| | | | |

**7 DIVISIONS** antérieures à la présente demande n° date n° date

**8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE** (nom et qualité du signataire)

Dominique DUPUIS-LATOUR
Avocat à la Cour

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

N/REF : 464-I 51247-FR

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION, CERTIFICAT D'UTILITE

## DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)


DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30


N° D'ENREGISTREMENT NATIONAL

98 12770

TITRE DE L'INVENTION :

Prodédé d'échange de données entre un automate et un objet portatif, notamment une carte à microcircuit, susceptible d'être débité par l'automate en contrepartie de la délivrance d'un bien ou d'un service.

LE(S) SOUSSIGNÉ(S)

Dominique DUPUIS-LATOUR
Avocat à la Cour
Cabinet BARDEHLE, PAGENBERG & PARTNER
45, avenue Montaigne
75008 - PARIS

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

GRIEU François
8, rue de Rambouillet
75012 - PARIS
FRANCE

MARDINIAN Grégory
13 Ter, rue de la République
95160 MONTMORENCY
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Dominique DUPUIS-LATOUR
Avocat à la Cour

BA 1102/7110R

La présente invention concerne les systèmes de transaction automatique délivrant un bien ou un service par l'intermédiaire d'un automate échangeant des informations avec un objet portatif débité d'une valeur ou montant donné en contrepartie du bien ou du service délivré.

L'automate peut être un distributeur automatique, par exemple de confiseries ou de boissons, ou un dispositif établissant un service, par exemple un contrôle d'accès matérialisé par l'ouverture d'un portillon pour le passage d'un voyageur dans un système de transport. Par la suite, on parlera de "délivrance d'un bien" pour simplifier, mais que l'invention vise bien entendu des applications beaucoup plus larges incluant la délivrance de toutes sortes de services.

De la même façon, on prendra l'exemple, comme objet portatif, d'une carte à microcircuit. Mais l'invention peut également être appliquée à d'autres types d'objets portatifs, tels que carte magnétique ou titre de transport, par exemple sous la forme d'un coupon magnétique ou analogue. L'utilisation d'une carte à microcircuit est cependant la mise en œuvre préférentielle compte tenu du très haut degré de sécurité et de fiabilité permis par cette technique.

La délivrance du bien ou du service résulte de la réalisation d'une transaction au cours de laquelle la carte est couplée temporairement à l'automate pour permettre un échange d'informations entre ces deux éléments, le paiement étant, au moins pour partie, réalisé par la modification d'une information stockée dans la mémoire de la carte, représentative de la valeur de cette dernière.

Le couplage entre carte et automate peut être réalisé par divers modes de liaison connus, avec ou sans contact galvanique, mais on verra que l'invention s'applique très avantageusement au couplage du type "sans contact". Dans ce mode de couplage, il existe en effet un risque non négligeable de rupture inattendue de la communication entre carte et automate, par exemple du fait de la sortie de la carte du rayon d'action de l'automate avant la fin du traitement, ou du fait d'une perturbation passagère, par exemple le passage d'une masse métallique à proximité, ou encore lorsque l'utilisateur passe trop rapidement sa carte devant le terminal pour permettre un échange satisfaisant des informations.

L'événement interrompant la transaction peut être aussi bien accidentel

que provoqué, par exemple intentionnellement par l'utilisateur afin d'obtenir la délivrance du bien tout en empêchant le débit de sa carte du montant correspondant.

L'un des buts de l'invention est, dans le cadre d'un système de transaction automatique tel qu'exposé ci-dessus, de lier le paiement (c'est-à-dire le débit de la carte) avec la délivrance du bien de manière à préserver aussi bien les intérêts de l'acheteur (utilisateur) que ceux du vendeur (le gestionnaire de l'automate), même si un événement interrompt la transaction ou empêche la réalisation du paiement.

Jusqu'à présent, le problème est habituellement traité de l'une des manières suivantes :

- on l'ignore sur le plan technique, quitte à le traiter par une procédure humaine ;
- on met temporairement la carte à l'abri d'un retrait par l'utilisateur, et l'automate opère le débit si, et seulement si, le bien est délivré (cas par exemple des automates dans lesquels la carte est occultée par un volet ou "avalée" pendant la transaction) ;
- la carte reste accessible à l'acheteur : on évite ainsi un élément mécanique coûteux, qui ralentit la transaction et se révèle en tout état de cause impraticable dans les transactions sans contact. Mais des précautions particulières doivent alors être prises.

La troisième situation, dans laquelle la carte reste physiquement accessible à l'utilisateur, aboutit à l'une ou l'autre des situations suivantes :

- débit opéré postérieurement à la délivrance du bien : l'acheteur peut essayer d'empêcher le débit, par exemple en retirant sa carte immédiatement après la délivrance du bien ou en rendant d'une autre manière le débit impossible (par exemple en isolant par un morceau d'adhésif l'une des plages de contact du microcircuit de la carte) ; cette manière de procéder est acceptable si la délivrance est intrinsèquement étalée dans le temps, par exemple une communication téléphonique, l'intérêt de la fraude étant très limité ; en revanche, elle n'est pas satisfaisante lorsque l'automate distribue un article, ou débloque un portillon.
- débit préalable à la délivrance du bien : il existe alors un risque que l'acheteur soit lésé, du fait de la réalisation du paiement par échange

d'informations à travers un canal de communication qui peut être interrompu par extraction ou éloignement de la carte ; en effet, il est possible que la carte soit débitée mais, l'automate n'en ayant pas la confirmation, il ne délivrera pas le bien.

L'invention se place dans le cadre général correspondant à cette dernière situation, c'est-à-dire celle dans laquelle la carte est débitée avant délivrance du bien.

La transaction, dans son aspect le plus général se déroule de la manière suivante :

10) l'automate commande le débit de la carte ;

20) la carte modifie l'information de valeur monétaire (ou une valeur équivalente en "jetons") ;

30) la carte confirme à l'automate la réalisation effective du débit, c'est-à-dire de la modification de la valeur monétaire dans la mémoire ;

40) l'automate délivre le bien.

Comme on le comprend aisément, une interruption de l'échange entre carte et automate intervenant au cours de l'étape 30 lèse l'acheteur.

Pour pallier cet inconvénient, on avait jusqu'à présent recours à diverses pratiques telles que :

- considérer que l'acheteur est fautif s'il retire sa carte pendant la transaction, et peut donc être pénalisé ; en cas de réclamation, on prévoit des procédures d'indemnisation plus ou moins arbitraires ou la création d'un moyen pour savoir a posteriori si la transaction inscrite dans la carte a été effectivement suivie d'effet par l'automate ;
- débiter des petits montants au fur et à mesure de la délivrance du bien à l'acheteur, en considérant que si l'acheteur est lésé, il le sera d'un montant faible et donc acceptable : cette solution convient parfaitement à la délivrance de fluides ou à une communication téléphonique, mais elle est impraticable pour la délivrance d'articles ou l'accès à un réseau de transport ;
- prévoir un système tel que, si la transaction courante est interrompue avec préjudice pour l'acheteur, dans une transaction ultérieure "de reprise" la délivrance du bien pourra avoir lieu sans nouveau paiement, c'est-à-dire sans nouveau débit de la carte.

Cette troisième solution est une pratique connue, utilisée par exemple

dans les porte-monnaie électroniques tels que ceux du projet de norme européenne EN 1546.

Dans ces systèmes connus, si le paiement a eu lieu, si l'utilisateur qui n'a pas obtenu une délivrance du bien désiré recommence la transaction sur le même automate, et si cette nouvelle transaction (transaction de reprise) se poursuit à son terme, le bien est délivré moyennant un paiement équitable.

Ces systèmes connus à transaction de reprise ont cependant en commun un inconvénient.

En effet, si la communication entre l'automate et la carte est interrompue pendant l'étape 30 ci-dessus, et que l'acheteur ne rétablit pas la liaison entre sa carte et le même automate, il sera lésé.

En particulier, quand il existe à proximité plusieurs automates délivrant un bien ou service identique (par exemple plusieurs portillons d'accès à un réseau de transport) le client qui, par exemple, passe un peu trop vite sa carte sans contact et constate la non-ouverture du portillon, va souvent tenter sa chance sur le portillon voisin, donc sur un autre automate que celui avec lequel il avait entamé la transaction initiale. Le second automate va le débiter, même si le premier avait déjà opéré un débit, de sorte que l'acheteur sera débité deux fois pour un seul bien ou service délivré (une seule ouverture de portillon).

Il est possible de pallier cet inconvénient en reliant ensemble les automates d'une même zone par un réseau permettant l'échange des informations utiles pour la reprise de la transaction; par exemple un numéro d'identification de la carte, le numéro du dernier automate ayant commandé un débit, le numéro de transaction correspondant pour cet automate, etc., de sorte que la reprise de la transaction soit possible sur l'un quelconque des automates du réseau.

L'utilisation d'un tel réseau présente deux inconvénients, en particulier :

- la nécessité d'un réseau, avec ses contraintes matérielles et logicielles,
- le fait que chaque automate doit interroger le réseau systématiquement avant d'ordonner le débit d'une carte (étape 10 ci-dessus), ce qui ralentit la transaction, ou bien que chaque automate doit stocker localement les informations relatives aux transactions non terminées

opérées (au moins récemment) par les autres automates du réseau et rechercher rapidement si la carte qu'il va débiter coïncide avec l'une de ces informations.

L'invention propose une solution au problème ci-dessus, qui évite ou minimise le recours à un réseau, avec des caractéristiques qui permettent de répondre aux contraintes les plus critiques, telles que celles des transactions par carte sans contact dans le domaine des transports, où chaque transaction :

- ~~doit être rapide (0,1 seconde environ) ;~~
- est susceptible d'être interrompue sans faute de l'utilisateur (geste trop rapide ou imprécis) ;
- met en jeu plusieurs lignes de péage (plusieurs portillons) entre lesquels l'acheteur peut se déplacer rapidement (1 à 2 secondes pour aller d'un portillon au voisin) ; et
- doit fonctionner de manière satisfaisante en cas de panne d'un quelconque de ces éléments, en particulier du réseau reliant les automates, si un tel réseau existe.

À cet effet, l'invention propose un procédé d'échange de données entre la mémoire non volatile d'un objet portatif, notamment d'une carte à microcircuit, et un automate auquel la carte est couplée temporairement pour permettre la délivrance d'un bien ou d'un service, la carte comportant une information de valeur susceptible d'être débitée par l'automate en contrepartie de ladite délivrance du bien ou service, caractérisé en ce qu'il comprend des étapes dans lesquelles l'automate commande la modification d'un indicateur de ratification, conservé dans la mémoire non volatile de la carte, entre deux états, à savoir un état ratifié correspondant au cas où la précédente transaction opérée avec la carte, indifféremment avec ledit terminal ou avec un autre, s'est déroulée correctement, et un état non ratifié dans le cas où cette précédente transaction a été interrompue en cours d'exécution, et dans lequel l'automate, successivement : débite conditionnellement la carte, si l'indicateur est à l'état ratifié ; commande le positionnement par la carte de l'indicateur à l'état non ratifié si un débit a été opéré à l'étape précédente ; commande ensuite la délivrance du bien ou du service ; et, si le bien est effectivement délivré à l'étape précédente, commande le positionnement par la carte de l'indicateur à l'état ratifié.

Le procédé peut notamment comprendre les étapes suivantes : a) par l'automate, lecture de l'état de l'indicateur de ratification et saut à l'étape (e) si celui-ci est à l'état non ratifié ; b) par l'automate, commande du débit de la carte d'un montant correspondant au bien ou service à délivrer ; c) par la carte, enregistrement du débit par mise à jour de l'information de valeur, et positionnement de l'indicateur à l'état non ratifié ; d) par la carte, confirmation à l'automate de l'enregistrement du débit ; e) par l'automate, délivrance du bien ou service ; f) par l'automate, commande du positionnement de l'indicateur à l'état ratifié ; et g) par la carte, modification de l'état de l'indicateur, pour le mettre à l'état ratifié.

Selon un certain nombre de caractéristiques subsidiaires avantageuses :

- le débit conditionnel de la carte est subordonné en outre à l'écoulement d'un délai depuis la précédente opération de positionnement de l'indicateur à l'état non ratifié et/ou à l'appartenance de l'automate exécutant la transaction courante à un groupe auquel appartient également l'automate ayant réalisé la transaction précédente ;
- lorsque l'indicateur est à l'état non ratifié, la délivrance sans débit est inhibée si l'automate détecte qu'une délivrance a eu lieu lors de la précédente utilisation de la carte ;
- le débit de la carte et le positionnement de l'indicateur à l'état non ratifié sont opérés de manière indivisible ;
- au moins une partie des informations modifiant l'état de la carte, notamment les commandes permettant de positionner l'indicateur à l'état ratifié, et/ou moins une partie des informations relatives à l'état de la carte, en particulier l'état de l'indicateur et la confirmation de la prise en compte du débit, sont préalablement traitées par des moyens cryptographiques conjointement mis en œuvre par la carte et l'automate ;
- la délivrance du bien ou du service est opérée de manière différée après une temporisation donnée ; on peut avantageusement prévoir alors que le bien soit délivré avant l'expiration de la temporisation en cas de confirmation de la bonne exécution de l'étape de positionnement par la carte de l'indicateur à l'état ratifié et/ou, par ailleurs, en insérant dans la transaction une pause de durée aléatoire ;
- les informations échangées entre l'automate et la carte sont chiffrées d'une manière empêchant de révéler le moment où est commandé par

l'automate, et réalisé par la carte, le positionnement de l'indicateur à l'état ratifié ;

- il est prévu un comptage cumulatif, dans l'automate, des occurences de lecture d'un indicateur à l'état non ratifié ;
- il est prévu un comptage cumulatif, dans la carte, des occurences de mémorisation de l'indicateur à l'état non ratifié entre deux transactions, des moyens pouvant notamment être prévus pour signaler le dépassement d'un seuil donné du comptage dans la carte, notamment des moyens pour inhiber la délivrance consécutive du bien ou du service ;
- la mémoire de la carte comporte une information de nature du bien ou service à délivrer, information mise à jour avant délivrance éventuelle de ce bien ou service.

D'autres caractéristiques et avantages ressortiront de la description ci-dessous d'un exemple de mise en œuvre de l'invention.

## Exemple

On va tout d'abord expliquer la manière dont est constitué un système avec transaction de reprise selon l'art antérieur (proche notamment du projet de norme EN 1546 de porte-monnaie électronique, mais transposable à un grand nombre d'autres applications).

Chaque carte possède dans sa mémoire :

a) un numéro d'identification de carte, invariable et caractéristique,
b) le numéro du dernier automate ayant commandé un débit dans la carte,
c) le numéro de transaction pour cet automate, et
d) la valeur de la carte, c'est-à-dire le montant monétaire ou son équivalent en jetons, qui est la donnée sur laquelle est opérée le débit.

Chaque automate, quant à lui, possède dans sa mémoire :

A) le numéro de la dernière carte à laquelle il a commandé un débit,
B) un numéro d'identification d'automate invariable et caractéristique,
C) un numéro de transaction, incrémenté par l'automate à chaque transaction.

La transaction comprend essentiellement les étapes suivantes :

05) l'automate lit dans la carte les informations a, b et c et détermine si

a = A, b = B et c = C ; dans l'affirmative, il passe directement à l'étape 40.

10) l'automate commande le débit de la carte du montant D correspondant au bien à délivrer, ainsi que l'écriture dans la carte de a = A, b = B et c = C.

20) la carte enregistre le débit, c'est-à-dire remplace d par (d-D) et a, b et c par les valeurs communiquées A, B, C.

30) la carte confirme à l'automate l'enregistrement du débit ;

40) l'automate délivre le bien et remplace C par C+1.

La transaction comporte bien entendu des étapes liées à l'établissement, au déroulement et à la conclusion de la communication entre l'automate et la carte, des étapes assurant la comptabilisation des sommes perçues par l'automate, et des étapes de génération et de vérification de certificat cryptographiques nécessaires pour s'assurer de l'authenticité des valeurs échangées. Ces étapes, en elles-mêmes connues, ne sont pas impliquées, sauf indication contraire, dans la mise en œuvre de l'invention, et ne seront pas décrites plus en détail.

On prévoit également des étapes permettant de gérer le cas où la valeur de la carte est insuffisante, et un traitement adapté pour arrêter les opérations : par exemple, la valeur de la carte est lue au préalable par l'automate, comparée au montant de la transaction, et l'étape 10 est inhibée en cas de crédit insuffisant ; on peut également prévoir, en variante ou en complément, que la carte effectue ce même contrôle et inhibe les étapes 20 et 30.

Par ailleurs, les diverses opérations effectuées à l'étape 20 sont avantageusement réalisées de manière indivisible, c'est-à-dire que l'on prévoit dans la carte des moyens tels que, si l'étape 20 est interrompue, une lecture ultérieure révélera les informations a, b, c et d soit toutes inchangées, soit toutes changées conformément aux commandes de l'automate, mais en aucune façon seulement certaines d'entre elles auront été modifiées.

Comme on l'a indiqué plus haut, en cas d'interruption de la communication entre l'automate et la carte pendant l'étape 40, si l'utilisateur effectue un réessai sur un automate qui n'est pas le même automate que celui de la transaction initiale interrompue, le second automate va débiter la carte,

même si le premier automate l'avait déjà fait. L'acheteur, débité deux fois pour un seul bien délivré, sera donc lésé par la transaction de reprise.

Pour pallier cette difficulté, et offrir un compromis acceptable entre l'assurance que l'acheteur ne sera pas lésé et la possibilité de fraude, l'invention prévoit essentiellement dans la mémoire de la carte un bit $\mathcal{R}$ qui sera appelé "bit de ratification", susceptible de prendre les deux états suivants (étant bien entendu qu'il est possible de permuter les rôles joués par les valeurs 0 et 1)

État 0 ("ratifié") : cas normal, la précédente transaction de l'utilisateur s'est bien déroulée, l'automate délivrera ultérieurement le bien en débitant la carte.

État 1 ("non ratifié") : la transaction précédente ne s'est pas terminée correctement (le bien n'a pas été délivré), et le bien devra être délivré ultérieurement sans débit de la carte.

S'il y a lieu de débiter la carte, l'indicateur est positionné à l'état 1 par l'automate avant délivrance du bien, et si le bien est ensuite délivré, l'automate commande le positionnement de $\mathcal{R}$ à l'état 0.

Plus précisément, la transaction comprend les étapes suivantes :

05) l'automate lit dans la carte l'état de $\mathcal{R}$ ; si celui-ci est à l'état 1, alors l'automate passe directement à l'étape 40 ;

10) l'automate commande le débit de la carte du montant D correspondant au bien délivré ;

20) la carte enregistre le débit, c'est-à-dire qu'elle remplace le solde d par (d-D) et positionne $\mathcal{R}$ à l'état 1 ;

30) la carte confirme à l'automate l'enregistrement du débit ;

40) l'automate, qui a reçu la confirmation de l'étape 30, ou via le test de l'étape 05, délivre le bien ;

45) l'automate commande le positionnement de $\mathcal{R}$ à l'état 0 ;

50) la carte modifie l'état de $\mathcal{R}$, qui passe à l'état 0.

Comme on peut le constater, le débit est opéré aux étapes 10, 20 et 30.

Dans le cas particulier où l'on débite des unités, on a D = 1, qui peut être dans ce cas implicite ; un autre cas particulier est celui à usage unique, correspondant à d = 1, puis d = 0, d pouvant être réduit à un unique élément binaire.

On remarquera que l'acheteur n'est jamais lésé lorsqu'en l'absence de

délivrance du bien il tente la même transaction par réessai sur un autre automate (a fortiori sur le même), et ce de manière caractéristique sans qu'il soit nécessaire d'établir un réseau entre automates.

On va maintenant décrire divers perfectionnements au procédé que l'on vient d'exposer.

Certains de ces perfectionnements visent notamment à réduire la probabilité d'une situation dans laquelle les étapes 05 à 45 se déroulent normalement, mais la transaction est interrompue juste après l'étape 45, empêchant la réalisation de l'étape 50.

Dans ce cas, l'acheteur, à qui l'automate a délivré le bien (étape 40), peut de fait disposer à nouveau du bien par une nouvelle transaction, sans être débité une seconde fois. Il y est donc de son intérêt d'empêcher l'exécution de l'étape 50, par exemple en passant volontairement la carte rapidement auprès de l'automate pour pouvoir interrompre la transaction juste après l'exécution de l'étape 45.

Un *premier perfectionnement* consiste, à l'étape 05, à passer à l'étape 40 (deuxième branche de l'alternative après test de l'état de $\mathcal{R}$) seulement si d'autres conditions que $\mathcal{R}$ égal 1 sont réunies, telles qu'en particulier le délai écoulé depuis le positionnement de $\mathcal{R}$ à 1 et/ou l'identité de l'automate ayant auparavant positionné l'indicateur.

Pour cela, on associe à l'indicateur, dans la carte, des informations caractéristiques de l'heure et/ou de la nature de l'automate qui a effectué le débit précédent (et/ou commandé le positionnement de l'indicateur) lors d'une précédente transaction. Ces informations sont avantageusement écrites lors de l'étape 20 (de la même manière qu'à l'étape 20 d'une transaction de l'art antérieur, décrite plus haut).

On compare ces informations mémorisées dans la carte à des informations correspondantes, caractéristiques de l'heure courante et/ou de la nature de l'automate qui s'apprête à délivrer le bien.

A titre d'exemple, dans une application au transport, ce perfectionnement a pour effet de ne permettre la reprise de la transaction avec un avantage indu de l'acheteur que si la précédente opération a commencé à s'exécuter sur la même ligne de péages et dans un délai assez faible pour exclure une réutilisation pour un nouveau trajet. Avec cette précaution, un voyageur ne peut effectuer deux trajets pour le prix d'un, et l'éventuelle

ouverture du portillon à un second voyageur (qui présente de nouveau le titre de transport non ratifié du premier voyageur) ne nuit pas davantage au transporteur qu'un franchissement en force du portillon, dans la mesure où de toute façon l'un des deux voyageurs n'est pas en règle en cas de contrôle.

Un *deuxième perfectionnement* consiste, à l'étape 05, à inhiber le passage à l'étape 40 (deuxième branche de l'alternative après test de l'état de $\mathcal{R}$) si l'automate a précédemment réalisé, pour cette même carte, une transaction qui a été poursuivie jusqu'à la bonne exécution de la délivrance. Ce perfectionnement a pour effet d'obliger en tout état de cause l'acheteur à changer d'automate pour avoir l'espoir d'obtenir une double délivrance.

L'automate procède à cette détection par exemple en consultant un historique des transactions qu'il a réalisées, comportant pour chaque transaction un identificateur de la carte et l'indication si la délivrance a eu lieu ; cet historique peut être partagé entre plusieurs automates, si un réseau de communication les relie (remarque : dans une application au péage la défaillance de ce réseau n'entraîne qu'une légère augmentation de la probabilité qu'un titre de transport soit utilisable sur un second portillon).

L'inhibition du paiement gratuit peut se traduire soit par l'arrêt de la transaction (cas du transport en cas de seconde utilisation dans le délai du premier perfectionnement ci-dessus) soit par une autre délivrance moyennant un nouveau paiement (cas de la délivrance d'un article).

Un *troisième perfectionnement* consiste, à l'étape 20, à effectuer le débit et la modification de l'indicateur $\mathcal{R}$ (ainsi que, le cas échéant, l'écriture des informations associées au premier perfectionnement visé plus haut) d'une manière telle que ces opérations soient indivisibles.

En d'autres termes, on prévoit dans la carte des moyens tels que, si l'étape 20 est interrompue, une lecture ultérieure révélera les informations $\mathcal{R}$ et d (et le cas échéant les informations associées au premier perfectionnement) soit toutes inchangées, soit toutes changées, conformément aux commandes de l'automate.

On évite ainsi certaines possibilités d'erreur, en faveur de l'acheteur ou de l'automate selon celle des opérations qui se serait opérée sans l'autre.

À titre d'exemple de réalisation (permettant de minimiser le nombre d'écri-

tures en mémoire), la carte comporte deux zones de mémoire $Z_0$ et $Z_1$ contenant chacune $R_i$, le solde $d_i$, un numéro $n_i$ pouvant prendre la valeur 0 ou 1 et une somme de contrôle $s_i$ portant sur $d_i$ et $n_i$ ($s_i$ est normalement le nombre de bits à 0 dans $d_i$ et $n_i$).

Préalablement à une lecture (en particulier à l'étape 05), la carte détermine laquelle des zone $Z_0$ ou $Z_1$ est valide, et à cette fin contrôle pour chacune des deux zones la validité de $s_i$ relativement à $d_i$ et $n_i$. Si $s_i$ est invalide, la carte ignore ou efface l'ensemble de la zone ; si, à l'issue de cette opération, une seule des deux zones est non ignorée ou effacée, alors cette zone est considérée comme valide ; si les deux zones sont non ignorées ou effacées la zone valide est donnée par la table suivante :

| $n_0$ | $n_1$ | zone valide |
|---|---|---|
| 0 | 0 | $Z_1$ |
| 1 | 0 | $Z_0$ |
| 1 | 1 | $Z_1$ |
| 0 | 1 | $Z_0$ |

Les valeurs retournées par la carte pour $\mathcal{R}$ (à l'étape 10) et d (pris en compte pour le calcul du nouveau solde à l'étape 20) sont $\mathcal{R}_i$ et $d_i$ de la zone valide.

L'écriture (étapes 20 et 50) aura lieu dans l'autre zone (après effacement préalable), avec une valeur de $n_i$ telle que la zone où aura lieu l'écriture devienne la zone valide, c'est à dire selon la table suivante :

| si zone valide | et | écriture en | et |
|---|---|---|---|
| $Z_1$ | $n_1 = 0$ | $Z_0$ | $n_0 = 1$ |
| $Z_0$ | $n_0 = 1$ | $Z_1$ | $n_1 = 1$ |
| $Z_1$ | $n_1 = 1$ | $Z_0$ | $n_0 = 0$ |
| $Z_0$ | $n_0 = 0$ | $Z_1$ | $n_1 = 0$ |

L'écriture dans cette zone se fera lors de l'étape 20 avec $\mathcal{R}_i = 1$, avant, ou simultanément avec, l'écriture de $n_i$, $d_i$ et $s_i$ ; à l'issue de cette écriture la zone valide a changé.

L'étape 50 écrit $\mathcal{R}_i = 0$ dans la zone valide.

L'écriture indivisible d'autres informations peut se traiter par extension des zones $Z_i$ et des données prises en compte par les sommes de contrôl $s_i$.

Un *quatrième perfectionnement* consiste à soumettre des informations

modifiant l'état de la carte, en particulier les commandes permettant de positionner l'indicateur de ratification à l'état 1, à la vérification préalable, par un dispositif intégré à la carte, de la validité d'un certificat cryptographique d'intégrité de message, produit dans l'automate par un moyen correspondant.

Un *cinquième perfectionnement* consiste, de façon symétrique du précédent, à soumettre des informations relatives à l'état de la carte, en particulier l'état de l'indicateur de ratification et/ou la confirmation de la prise en compte du débit, à la vérification préalable, par un dispositif intégré à l'automate, de la validité d'un certificat cryptographique d'intégrité de message, produit dans la carte par un moyen correspondant.

À titre d'exemple, le certificat cryptographique des quatrième et cinquième perfectionnements ci-dessus peut être une signature électronique de message obtenue et vérifiée selon la méthode de la norme ISO 9796-2, ou plus simplement selon un algorithme symétrique de type DES.

Un certain nombre d'autres perfectionnements visent à augmenter la difficulté, pour un utilisateur, d'interrompre sciemment la transaction.

Un *sixième perfectionnement* consiste ainsi à modifier l'étape 40 en remplaçant la délivrance pure et simple du bien par une décision d'opérer ou non cette délivrance après une temporisation. Pour améliorer la rapidité de ce système, on peut délivrer le bien avant expiration de la temporisation si l'automate a la confirmation de la bonne exécution de l'étape 50, au lieu d'attendre l'expiration de la temporisation. Ces précautions rendent infructueuses les éventuelles tentatives de l'acheteur d'empêcher l'étape 50 en interrompant la communication immédiatement après la délivrance.

Le séquencement est ainsi modifié (étant observé que les étapes 40 et 45 peuvent être inversées) :

40) l'automate lance une temporisation,

45) étape inchangée,

50) étape inchangée,

55) la carte acquitte l'exécution de l'étape 50 par émission d'un message spécifique (étape facultative, mais permettant d'écourter la durée moyenne de la transaction),

60) l'automate délivre le bien à l'expiration du temporisateur ou, le cas échéant, à la réception du message de l'étape 55, au premier des

deux termes échus. L'utilisateur est ainsi privé du repère temporel qui lui permettrait d'interrompre la transaction à son profit.

Un *septième perfectionnement* consiste à protéger contre l'écoute les communications entre l'automate et la carte par un moyen tel qu'un chiffrement cryptographique, de sorte que cette écoute ne puisse révéler le moment où l'écriture à 0 du bit de ratification $\mathcal{R}$ est commandée et exécutée. On rend ainsi plus difficile la détermination de l'instant où il serait avantageux d'interrompre la communication.

Un *huitième perfectionnement* consiste, en complément du sixième et/ou du septième perfectionnement précédent, à insérer dans la transaction une pause variant aléatoirement, toujours dans le but de rendre plus difficile la détermination de l'instant où il serait avantageux d'interrompre la communication. Cette pause à variation aléatoire est de préférence inséré dans une étape située avant le débit de la carte.

Un *neuvième perfectionnement* consiste à détecter une situation très vraisemblablement anormale, révélée par un trop grand nombre de transactions gratuites. À cet effet, un dispositif compteur adéquat compte les cas où à l'étape 05 la décision est prise de faire une délivrance sans paiement. On peut également totaliser les montants ainsi potentiellement perdus par les automates. Si ce compteur est intégré à l'automate, il aura des fins statistiques ; s'il est intégré à la carte, il est avantageux de subordonner la délivrance du bien ou du service à la confirmation de la bonne mise à jour du compteur dans le cas où l'acheteur échappe au débit, de sorte qu'il ne puisse, au moins, échapper à la mise à jour du compteur.

On peut prévoir un dispositif inhibant la délivrance du bien quand le compteur dépasse un seuil, ou bien une alarme ou signalisation analogue. On peut également prévoir un retour en arrière total ou partiel du compteur, par exemple à chaque transaction avec débit, ou avec un dispositif spécifique.

Un *dixième perfectionnement* consiste à enregistrer la nature du bien à délivrer, par exemple lors de l'étape 20, et à lire et utiliser cette information notamment quand, à l'issue de l'étape 05, la décision est prise d'effectuer une délivrance sans débit. Ceci permet de traiter la reprise de la transaction dans le cas d'automates capables de délivrer plusieurs types de bien, ou des montants différents, ou par exemple dans un système de

transport avec des destinations différentes en fonction d'une sélection par l'usager.

## REVENDICATIONS

1. Un procédé d'échange de données entre la mémoire non volatile d'un objet portatif, notamment d'une carte à microcircuit, et un automate auquel la carte est couplée temporairement pour permettre la délivrance d'un bien ou d'un service, la carte comportant une information de valeur susceptible d'être débitée par l'automate en contrepartie de ladite délivrance du bien ou service,
procédé caractérisé en ce qu'il comprend des étapes dans lesquelles l'automate commande la modification d'un indicateur de ratification, conservé dans la mémoire non volatile de la carte, entre deux états, à savoir un état ratifié correspondant au cas où la précédente transaction opérée avec la carte, indifféremment avec ledit terminal ou avec un autre, s'est déroulée correctement, et un état non ratifié dans le cas où cette précédente transaction a été interrompue en cours d'exécution,
et dans lequel l'automate, successivement :
- débite conditionnellement la carte, si l'indicateur est à l'état ratifié,
- commande le positionnement par la carte de l'indicateur à l'état non ratifié si un débit a été opéré à l'étape précédente,
- commande ensuite la délivrance du bien ou du service, et
- si le bien est effectivement délivré à l'étape précédente, commande le positionnement par la carte de l'indicateur à l'état ratifié.

2. Le procédé de la revendication 1, comprenant les étapes suivantes :
a) par l'automate, lecture de l'état de l'indicateur de ratification et saut à l'étape e) si celui-ci est à l'état non ratifié,
b) par l'automate, commande du débit de la carte d'un montant correspondant au bien ou service à délivrer,
c) par la carte, enregistrement du débit par mise à jour de l'information de valeur, et positionnement de l'indicateur à l'état non ratifié,
d) par la carte, confirmation à l'automate de l'enregistrement du débit,
e) par l'automate, délivrance du bien ou service,
f) par l'automate, commande du positionnement de l'indicateur à l'état ratifié, et
g) par la carte, modification de l'état de l'indicateur, pour le mettre à l'état

ratifié.

3. Le procédé de l'une des revendications précédentes, dans lequel le débit conditionnel de la carte est subordonné en outre à l'écoulement d'un délai depuis la précédente opération de positionnement de l'indicateur à l'état non ratifié.

4. Le procédé de l'une des revendications précédentes, dans lequel le débit conditionnel de la carte est subordonné en outre à l'appartenance de l'automate exécutant la transaction courante à un groupe auquel appartient également l'automate ayant réalisé la transaction précédente.

5. Le procédé de l'une des revendications précédentes, dans lequel, lorsque l'indicateur est à l'état non ratifié, la délivrance sans débit est inhibée si l'automate détecte qu'une délivrance a eu lieu lors de la précédente utilisation de la carte.

6. Le procédé de l'une des revendications précédentes, dans lequel le débit de la carte et le positionnement de l'indicateur à l'état non ratifié sont opérés de manière indivisible.

7. Le procédé de l'une des revendications précédentes, dans lequel au moins une partie des informations modifiant l'état de la carte, notamment les commandes permettant de positionner l'indicateur à l'état ratifié, sont préalablement traitées par des moyens cryptographiques conjointement mis en œuvre par la carte et l'automate.

8. Le procédé de l'une des revendications précédentes, dans lequel au moins une partie des informations relatives à l'état de la carte, en particulier l'état de l'indicateur et la confirmation de la prise en compte du débit, sont préalablement traitées par des moyens cryptographiques conjointement mis en œuvre par la carte et l'automate.

9. Le procédé de l'une des revendications précédentes, dans lequel la délivrance du bien ou du service est opérée de manière différée après une

temporisation donnée.

10. Le procédé de la revendication 9, dans lequel le bien est délivré avant l'expiration de la temporisation en cas de confirmation de la bonne exécution de l'étape de positionnement par la carte de l'indicateur à l'état ratifié.

11. Le procédé de la revendication 9, dans lequel il est inséré dans la transaction une pause de durée aléatoire.

12. Le procédé de l'une des revendications précédentes, dans lequel les informations échangées entre l'automate et la carte sont chiffrées d'une manière empêchant de révéler le moment où est commandé par l'automate, et réalisé par la carte, le positionnement de l'indicateur à l'état ratifié.

13. Le procédé de l'une des revendications précédentes, comprenant le comptage cumulatif, dans l'automate, des occurences de lecture d'un indicateur à l'état non ratifié.

14. Le procédé de l'une des revendications précédentes, comprenant le comptage cumulatif, dans la carte, des occurences de mémorisation de l'indicateur à l'état non ratifié entre deux transactions.

15. Le procédé de la revendication 13 ou 14, dans lequel il est prévu des moyens pour signaler le dépassement d'un seuil donné du comptage dans la carte, notamment des moyens pour inhiber la délivrance consécutive du bien ou du service.

16. Le procédé de l'une des revendications précédentes, dans lequel la mémoire de la carte comporte une information de nature du bien ou service à délivrer, information mise à jour avant délivrance éventuelle de ce bien ou service.